ESCAPE

European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures

ESCAPE IAM

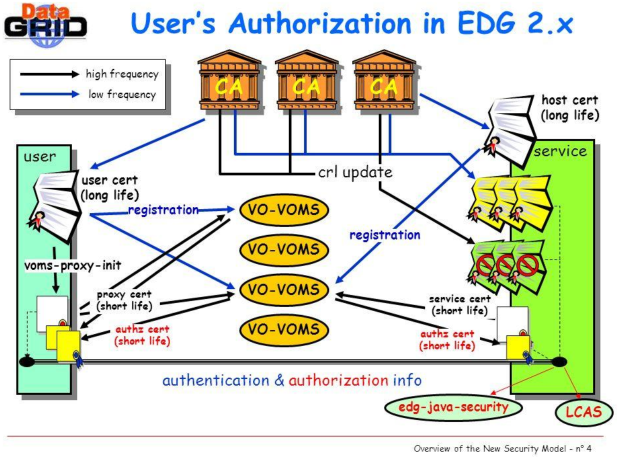
INFN-CNAF
Roberta Miccoli, Federica Agostini

E-OSSR Onboarding Presentation
15/06/2023

ESCAPE - The European Science Cluster of Astronomy & Particle Physics ESFRI Research Infrastructures has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement n° 824064.

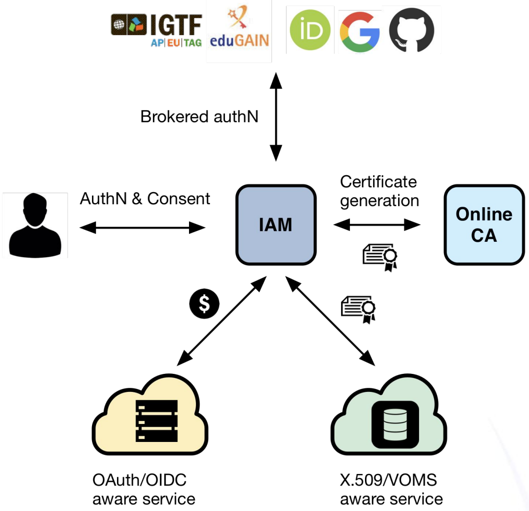
ESCAPE Data Lake AAI and WLCG

Current, X.509 based AAI



Move beyond X.509

Future, token-based AAI



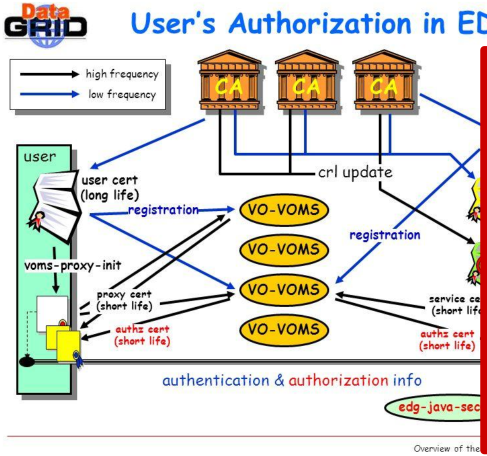
Approach: leverage and build upon the WLCG experience

Funded by the European Union's
Horizon 2020 - Grant N° 824064

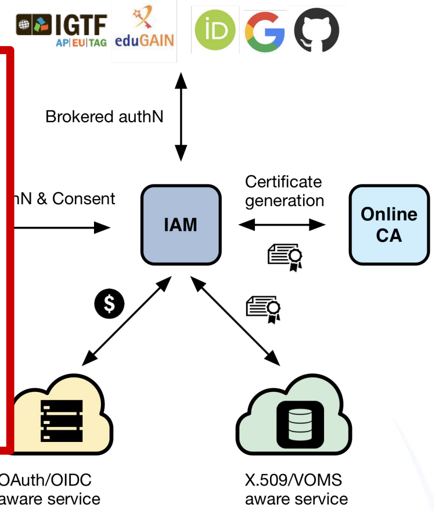
ESCAPE Data Lake AAI and WLCG

Current, X.509 based AAI

Future, token-based AAI



The transition will be gradual!

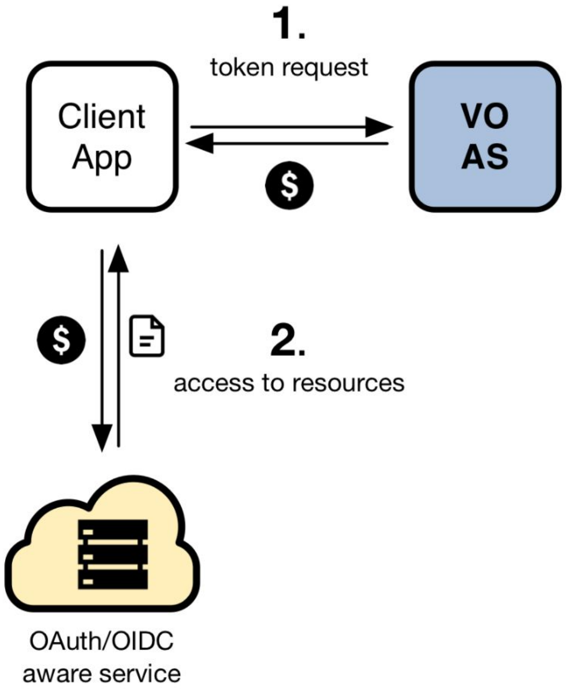


Approach: leverage and build upon the WLCG experience

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Token-based AuthN/Z

- In order to access resources/services, a **client application** needs an **access token**
- The token is obtained from **a Virtual Organization** (which acts as an OAuth Authorization Server) using standard **OAuth/OpenID Connect** flows
- **Authorization** is then **performed at the services** leveraging info extracted from the token:
  - **Identity attributes**: e.g., **groups**
  - **OAuth scopes**: capabilities linked to access tokens at token creation time



Funded by the European Union's Horizon 2020 - Grant N° 824064

In practice

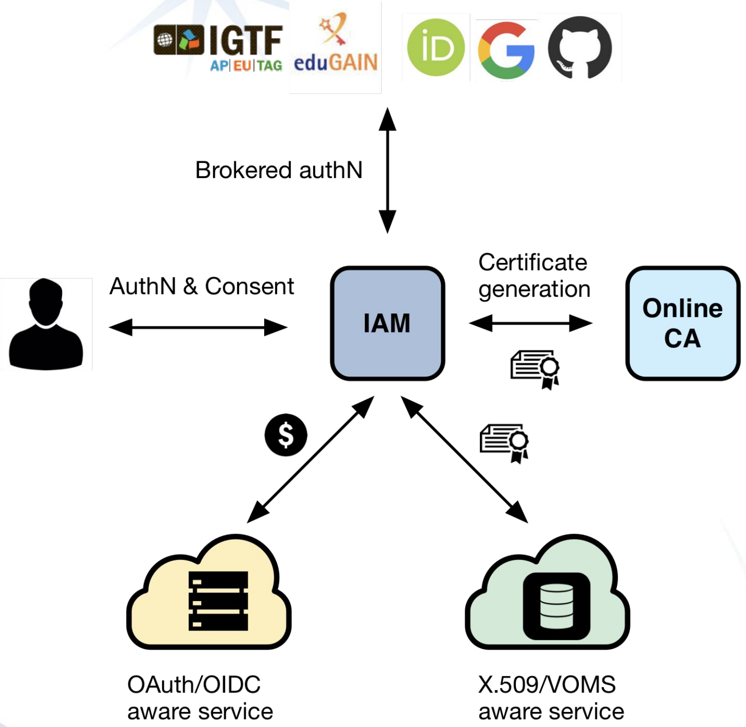
- The central authorization server provides **attributes** that can be used for authorization at services:
  - groups/roles, e.g.: **cms**, **lofar**, **production-manager**
  - capabilities, e.g.: **storage.read:/cms**, **submit-job**
- This information is exposed to services via **signed JWT tokens** and via **OAuth/OpenID Connect protocol message exchanges** (aka flows)
- Services can then grant or deny access to functionality based on this information. Examples:
  - allow read access on the **/cms** to all members of the **cms** group
  - allow read access on the **/lofar** namespace to anyone with the capability **storage.read:/lofar**

Funded by the European Union's
Horizon 2020 - Grant N° 824064

INDIGO Identity and Access Management Service

An authentication and authorization service that:

- supports **multiple authentication mechanisms**
- provides users with a **persistent, organization scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate existing **VOMS**-aware services
- supports **Web** and **non-Web access**, **delegation** and **token renewal**



Funded by the European Union's Horizon 2020 - Grant N° 824064

INDIGO Identity and Access Management Service

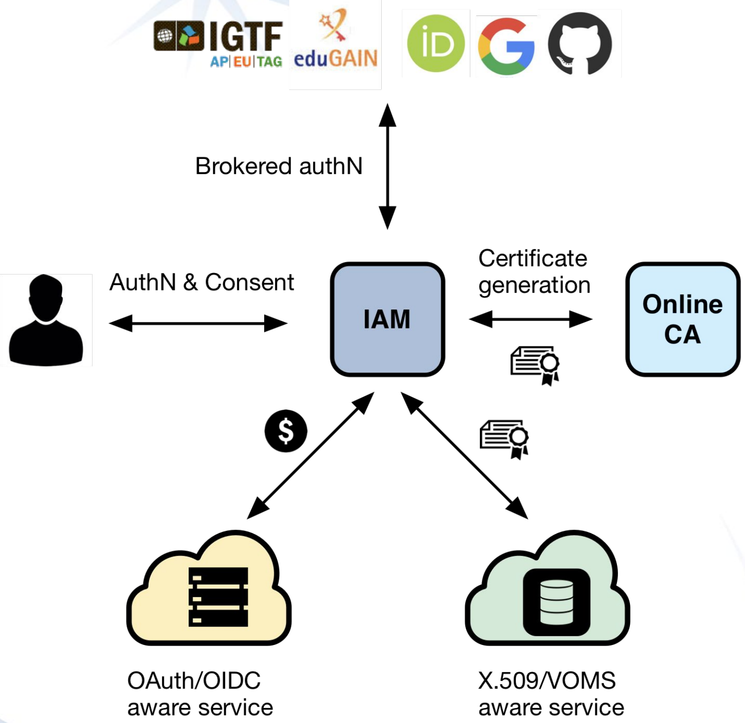
First developed in the context of the **H2020 INDIGO DataCloud** project

- ~7 years since 1st INDIGO IAM release v0.3.0 (2016-07-12)

Selected by the WLCG management board to be the core of the future, token-based WLCG AAI

Commitment by INFN for the foreseeable future, with current support from:

ESCAPE · EOSC Pillar · EGI-ACE · EOSC Future



Funded by the European Union's Horizon 2020 - Grant N° 824064

IAM supported OAuth grant types

- Authorization grant types, or authorization flows, are ways for an application to get tokens
- The supported grant types in IAM are
  - **authorization code** → mainly used by server-side web applications which can maintain the confidentiality of client credentials
  - **device code** → used by clients that can not easily trigger a browser-based authorization and could run on a separate device
  - **refresh token** → it allows an application to act on behalf of a user and get tokens without user's interaction

Funded by the European Union's
Horizon 2020 - Grant N° 824064

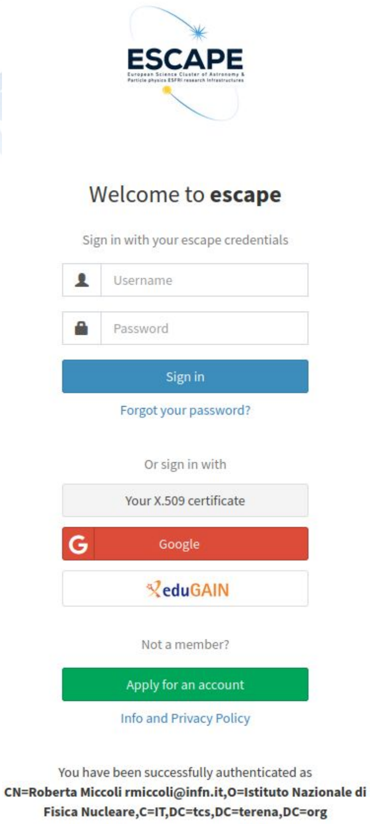
IAM supported OAuth grant types

- **client credentials** → used to obtain tokens not linked to user identities, since the client can make token requests by itself
- **token exchange** → satisfy the needs to access resources hosted by other downstream services on behalf of the user
- **implicit** (deprecated in OAuth 2.1) → it simplifies the authorization code flow, mainly used by client-side web applications
- **password** (deprecated in OAuth 2.1) → linked to user's credentials, does not support delegation

Funded by the European Union's Horizon 2020 - Grant N° 824064

The ESCAPE IAM instance

- ESCAPE IAM instance available
  - Root of trust for the ESCAPE Data Lake
  - 238 registered users
  - 18 groups
  - AuthN with EduGAIN, X.509 certificates, Google, username/password
  - currently at version **v1.8.1**
- VOMS endpoint available
- Registration open
  - Administrator-vetted registration flow
- Documentation available here



Welcome to **escape**

Sign in with your escape credentials

Or sign in with

Not a member?

You have been successfully authenticated as
CN=Roberta Miccoli rmiccoli@infn.it,O=Istituto Nazionale di Fisica Nucleare,C=IT,DC=tcs,DC=terena,DC=org

Funded by the European Union's Horizon 2020 - Grant N° 824064

INDIGO IAM - development

IAM core technologies

IAM is a **Spring Boot** application

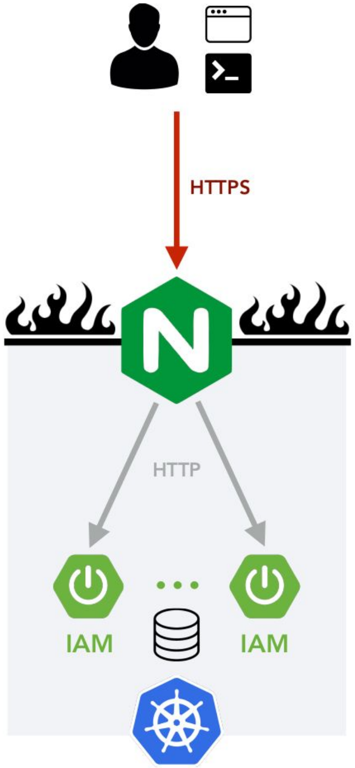
- currently based on the MitreID Connect
- deployed behind an **NGINX**
- stores data in a **MariaDB/MySQL** database

Horizontally scalable

- all state persisted in the database

We deploy IAM as a **containerized** service on top of **Kubernetes**

- autoscaling, zero downtime rolling updates



Funded by the European Union's
Horizon 2020 - Grant N° 824064

IAM APIs - a subset

- SCIM API - IAM provides a RESTful API, based on the **S**ystem for **C**ross-domain **I**dentity **M**anagement (**SCIM**) standard, that can be used to access information in the IAM database
  - users, groups, group memberships, etc…
  - The API can be used as an **integration point towards external systems**
    - for example, the SCIM API is used in the integration with the HTCondor batch system to do UNIX account pre-provisioning based on IAM account information

Funded by the European Union's Horizon 2020 - Grant N° 824064

IAM APIs - a subset

- IAM account API - it's a RESTful API used to manage user attributes, authorities, labels, clients, group membership, etc.
- **IAM client management & registration API** - this API solves several scalability and usability limits of old MITREid Connect API:
  - **pagination** → no pagination on MITREid client management APIs causes the management dashboard to be unavailable with a large number of clients
  - **server-side search functionality** → no client search API on MITREid
  - **clients ownership** → on MITREid managing a client requires to use registration access tokens, making it hard for users to have a clear view of their registered clients; now users own their created clients and old registration access token can be used to **redeem** and link an owned client

Funded by the European Union's
Horizon 2020 - Grant N° 824064

ESCAPE current release: IAM v1.8.1

Released on: **2023-02-28**

Major **highlights**:

- Scopes management interface added to IAM dashboard
- Group Manager interface added to IAM dashboard
- Support for AARC-G069 guideline (groups and roles membership information can be requested with the `entitlements` scope and appears in the `entitlements` claim of the access token) to increase conformance to AARC Blueprint Architecture

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Latest release: IAM v1.8.2

Released on: **2023-05-31**

Major **highlights**:

- Introduced new admin scopes in order to access IAM API endpoints
  - From this release, an administrator access token is not enough to have full access to IAM API endpoints. The scopes **iam:admin.read** and **iam:admin.write** are now needed
- Bump Spring-Boot version to 2.6.14

Funded by the European Union's Horizon 2020 - Grant N° 824064

Our roadmap

In progress:

- Add scope policy management into IAM dashboard #382
- IAM username update blocked by case insensitive "is username available" check #434
- Case sensitivity confusion between MySQL unique fields and JPA equals comparisons #550

To do:

- Local accounts: check password quality #544
- Support for AARC guidelines #467, #466, #469
- Can't add certificate with same subject and different issuer #454
- Client problems due to unsupported response types #601
- IAM should allow users to request account removal #362
- Support for Multi-factor Authentication #418
- **Scalability/availability assessment**
- **Overall security assessment**
- **Support for OIDC Federation model**

…

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Support for AARC guidelines

Support for AARC guidelines

IAM support to the AARC Blueprint Architecture is currently based on the following guidelines:

- AARC-G002/AARC-G069 describe how to encode **group membership information**, in particular:
    - groups are not included by default in access and ID tokens
    - groups can be requested using the `eduperson_entitlement/entitlements`scope and they are encoded as URN in the `eduperson_entitlement/entitlements`claim
    - smooth transition between new and old claim: if users ask for the old `eduperson_entitlement` scope, they still get `eduperson_entitlement`claim in addition to the newest `entitlements` claim

Example:

```
$ oidc-token -s eduperson_entitlement aarc-client | jwt decode

"eduperson_entitlement": [
    "urn:geant:projectescape.eu:group:escape:cms",
    "urn:geant:projectescape.eu:group:escape"
  ]
"entitlements": [
    "urn:geant:projectescape.eu:group:escape:cms",
    "urn:geant:projectescape.eu:group:escape"
  ]
```

In the context of the ESCAPE project, `projectescape.eu` is a delegated namespace registered under *geant*

Funded by the European Union's
Horizon 2020 - Grant N° 824064

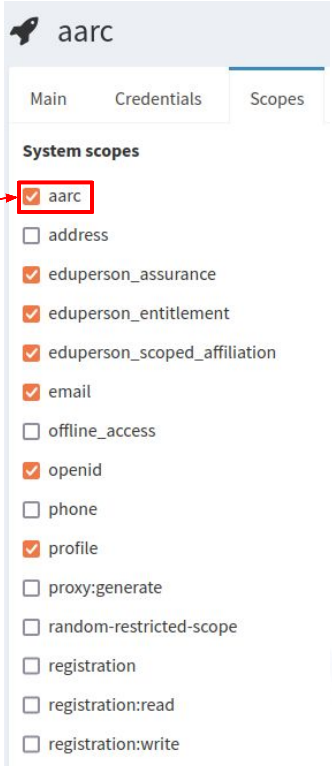
Support for AARC guidelines

- AARC-G021 for expressing assurance information
  - LoA can be requested using the `eduperson_assurance` scope and it is encoded in the `eduperson_assurance` claim
  - e.g. `"eduperson_assurance": ["https://refeds.org/assurance","https://refeds.org/assurance/IAP/low"]`
- AARC-G025 for expressing affiliation information within Community
  - Affiliation can be requested using the `eduperson_scoped_affiliation` scope and it is encoded in the `eduperson_scoped_affiliation` claim
  - e.g. `"eduperson_scoped_affiliation": "member@projectescape.eu"` (hardcoded in IAM v1.8.0)

Funded by the European Union's Horizon 2020 - Grant N° 824064

Enabling AARC support: the AARC profile

- An INDIGO IAM profile is a set of rules that can customize which information is included within:
  - access tokens
  - id tokens
  - userinfo endpoint responses
  - introspection endpoint responses
- The default JWT profile is `iam` but can be changed by configuration
- The configured default profile can be overridden per client:
  - clients must be configured to support **a scope equal to the name of the profile**
    - same logic used with the `openid` scope
  - example: a client requesting a token with the `eduperson_assurance` scope should request `scope="aarc eduperson_assurance "`
- IAM currently supports three profiles: `iam`, `wlcg` and `aarc`



aarc

Main | Credentials | Scopes

System scopes

☑ aarc
☐ address
☑ eduperson_assurance
☑ eduperson_entitlement
☑ eduperson_scoped_affiliation
☑ email
☐ offline_access
☑ openid
☐ phone
☑ profile
☐ proxy:generate
☐ random-restricted-scope
☐ registration
☐ registration:read
☐ registration:write

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Support for AARC guidelines - Future developments

We planned to work soon on supporting:

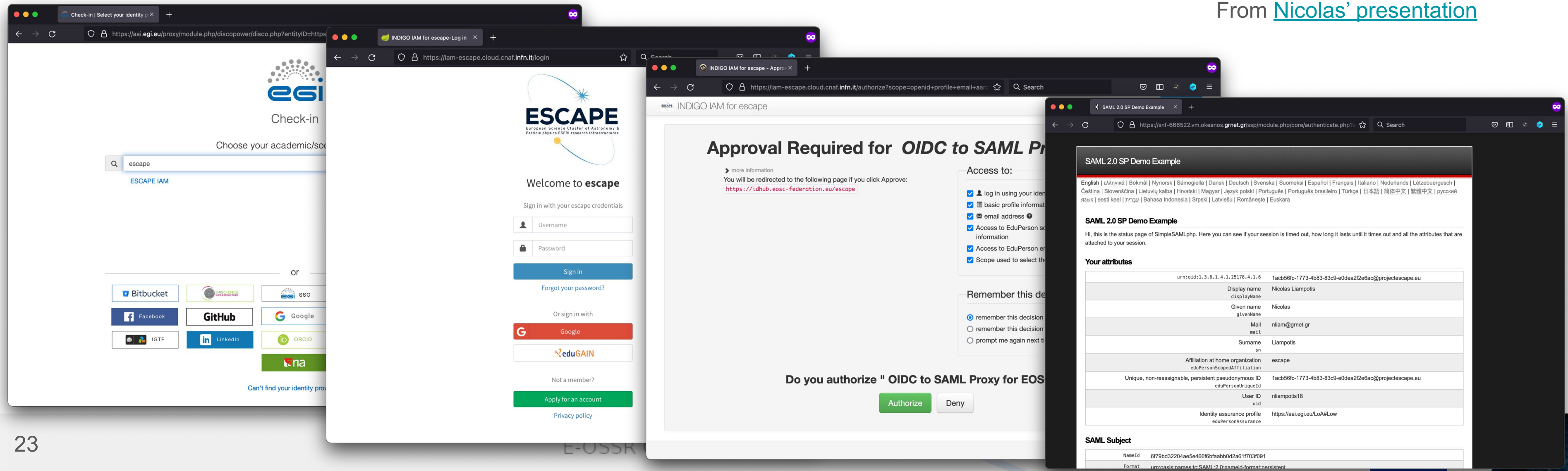
- AARC-G026 guideline
  - add voPersonID
- full support AARC-G025 guideline
  - now only eduPersonScopedAffiliation is defined
  - to-do: if logged via a remote provider, propagate its eduPersonScopedAffiliation to voPersonExternalAffiliation
- AARC-G049/AARC-G061 guideline
  - support aarc_idp_hint (ex idphint) to identify the supported SAML EntityID (or OIDC issuer)
- AARC-G031 guideline
  - support combination of the assurance of external identities

Funded by the European Union's
Horizon 2020 - Grant N° 824064

IAM integration with EGI Check-in

- Check-in acts as SAML Service Provider
- The ESCAPE IAM instance acts as SAML Identity Provider
  - since IAM can only act as SP, in order to integrate the ESCAPE IAM into the EOSC AAI federation an OIDC-to-SAML proxy has been deployed

From Nicolas' presentation



Check-in | Select your identity p

https://aai.egi.eu/proxy/module.php/discopower/disco.php?entityID=https

Check-in

Choose your academic/so

escape

ESCAPE IAM

or

Can't find your identity pro

INDIGO IAM for escape-Log in

https://iam-escape.cloud.cnaf.infn.it/login

ESCAPE European Science Cluster of Astronomy & Particle physics ESFRI research infrastructures

Welcome to escape

Sign in with your escape credentials

Username

Password

Forgot your password?

Or sign in with

Not a member?

Privacy policy

INDIGO IAM for escape - Approv

https://iam-escape.cloud.cnaf.infn.it/authorize?scope=openid+profile+email+aarc

INDIGO IAM for escape

Approval Required for *OIDC to SAML Pr*

› more information

You will be redirected to the following page if you click Approve:
`https://idhub.eosc-federation.eu/escape`

Access to:

☑ log in using your iden
☑ basic profile informat
☑ email address
☑ Access to EduPerson sc information
☑ Access to EduPerson en
☑ Scope used to select th

Remember this de

● remember this decision
○ remember this decision
○ prompt me again next ti

Do you authorize " OIDC to SAML Proxy for EOS

SAML 2.0 SP Demo Example

https://snf-666522.vm.okeanos.grnet.gr/ssp/module.php/core/authenticate.php?a

SAML 2.0 SP Demo Example

English | ελληνικά | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomeksi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עִבְרִית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

SAML 2.0 SP Demo Example

Hi, this is the status page of SimpleSAMLphp. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that are attached to your session.

Your attributes

urn:oid:1.3.6.1.4.1.25178.4.1.6	1acb56fc-1773-4b83-83c9-e0dea2f2e6ac@projectescape.eu
Display name displayName	Nicolas Liampotis
Given name givenName	Nicolas
Mail mail	nliam@grnet.gr
Surname sn	Liampotis
Affiliation at home organization eduPersonScopedAffiliation	escape
Unique, non-reassignable, persistent pseudonymous ID eduPersonUniqueId	1acb56fc-1773-4b83-83c9-e0dea2f2e6ac@projectescape.eu
User ID uid	nliampotis18
Identity assurance profile eduPersonAssurance	https://aai.egi.eu/LoA#Low

SAML Subject

NameId	6f79bd32204ae5e466f6bfaabb0d2a61f703f091
Format	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

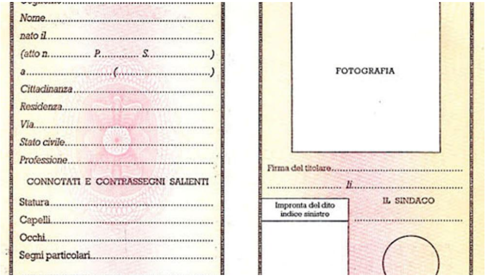
Future support for OIDC Federations

- The OpenID Connect Federation 1.0 specification, being finalised, describes how two entities wishing to interact can **dynamically** retrieve and resolve trust and metadata for a given protocol using a third-party *Trust Anchor*
- In SAML, a participant in several federations must create ad hoc metadata for each federation
- In OIDC-Fed, all federation participants publish their own federation metadata, which is the same for all federations to which the participant belongs; the final dynamically produced metadata is the result of the various policies acquired by the trust anchors applied to the entity metadata

Funded by the European Union's Horizon 2020 - Grant N° 824064

SAML vs OIDC Federation

SAML



Nome.................................

nato il...............................

(atto n............. P............ S.................)

a...............................(.....................)

Cittadinanza.......................

Residenza...........................

Via.....................................

Stato civile..........................

Professione.........................

CONNOTATI E CONTRASSEGNI SALIENTI

Statura................................

Capelli................................

Occhi..................................

Segni particolari..................

FOTOGRAFIA

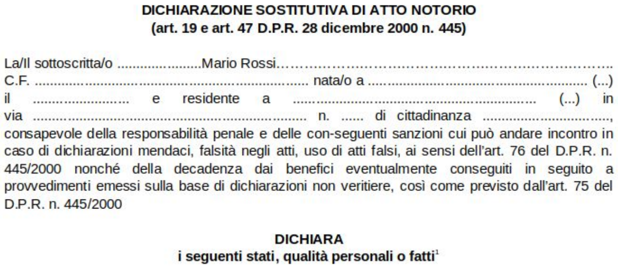
Firma del titolare.......................

.... il.............

Impronta del dito indice sinistro

IL SINDACO

OIDC Federation



DICHIARAZIONE SOSTITUTIVA DI ATTO NOTORIO
(art. 19 e art. 47 D.P.R. 28 dicembre 2000 n. 445)

La/Il sottoscritta/o ....Mario Rossi...
C.F. .... nata/o a .... (...)
il .... e residente a .... (...) in
via .... n. ...... di cittadinanza ....,
consapevole della responsabilità penale e delle con-seguenti sanzioni cui può andare incontro in caso di dichiarazioni mendaci, falsità negli atti, uso di atti falsi, ai sensi dell'art. 76 del D.P.R. n. 445/2000 nonché della decadenza dai benefici eventualmente conseguiti in seguito a provvedimenti emessi sulla base di dichiarazioni non veritiere, così come previsto dall'art. 75 del D.P.R. n. 445/2000

DICHIARA
i seguenti stati, qualità personali o fatti[1]

- **SAML**
  - the SAML metadata can be compared to the identity card of a Service Provider (SP)
  - the characteristic information of a service is certified by Federation Authority
- **OIDC Federation**
  - the Trust Anchor guarantees the identity of the federation members
  - federation member declares their characteristics
  - e.g. in the declaration in lieu of affidavit, Mario Rossi declares and signs his characteristics

Funded by the European Union's
Horizon 2020 - Grant N° 824064

IAM deployment, performance and HA

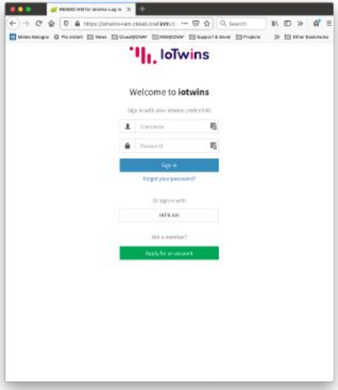
IAM deployments at CNAF

https://cta-lst.cloud.cnaf.infn.it/login

Welcome to **cta-lst @ INFN-CNAF**

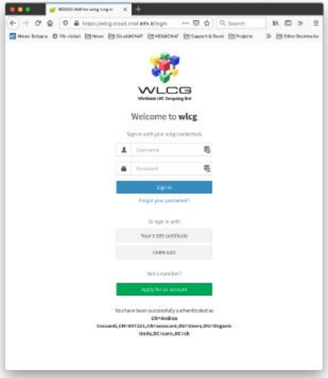
Sign in with

You have been successfully authenticated as **CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch**


https://iotwins-iam.cloud.cnaf.infn.it

Welcome to **iotwins**

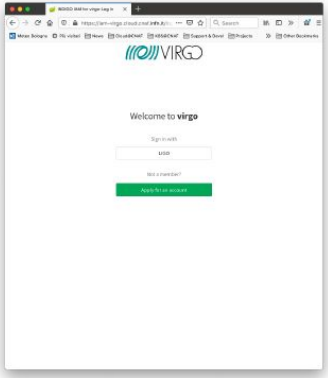
Sign in with your iotwins credentials


https://wlcg.cloud.cnaf.infn.it/login

Welcome to **wlcg**

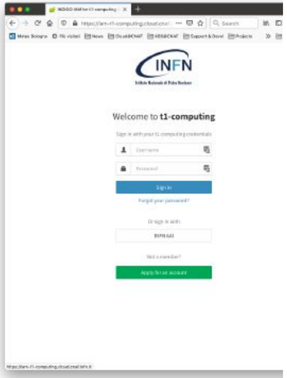
Sign in with your wlcg credentials

You have been successfully authenticated as **CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch**


https://iam-virgo.cloud.cnaf.infn.it/

Welcome to **virgo**

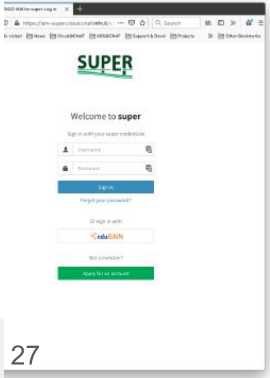
Sign in with


https://iam-t1-computing.cloud.cnaf.infn.it

Welcome to **t1-computing**

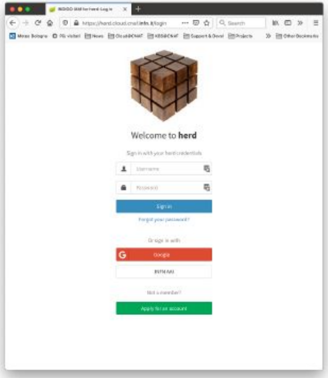
Sign in with your t1-computing credentials

~ 20 IAM instances


https://iam-super.cloud.cnaf.infn.it/

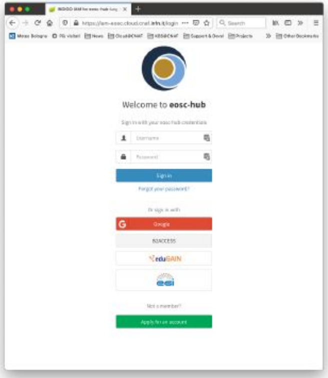
Welcome to **super**

Sign in with your super credentials


https://herd.cloud.cnaf.infn.it/login

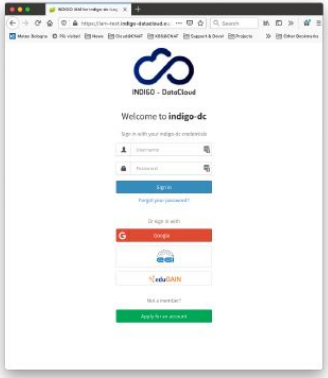
Welcome to **herd**

Sign in with your herd credentials


https://iam-eosc.cloud.cnaf.infn.it/login

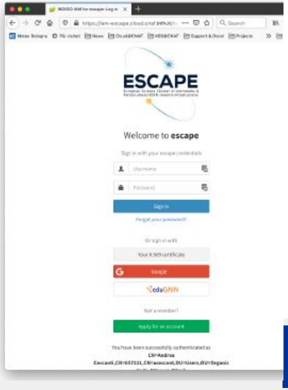
Welcome to **eosc-hub**

Sign in with your eosc-hub credentials


https://iam-test.indigo-datacloud.eu

Welcome to **indigo-dc**

Sign in with your indigo-dc credentials


https://iam-escape.cloud.cnaf.infn.it/

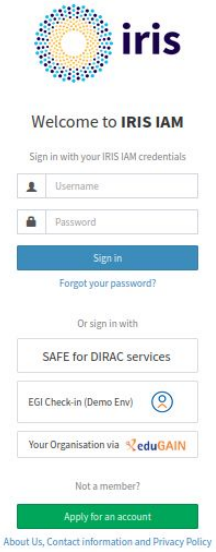
Welcome to **escape**

Sign in with your escape credentials

You have been successfully authenticated as **CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch**

IAM deployments outside CNAF

~ 10 IAM instances



Welcome to **IRIS IAM**

Sign in with your IRIS IAM credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

SAFE for DIRAC services

EGI Check-in (Demo Env)

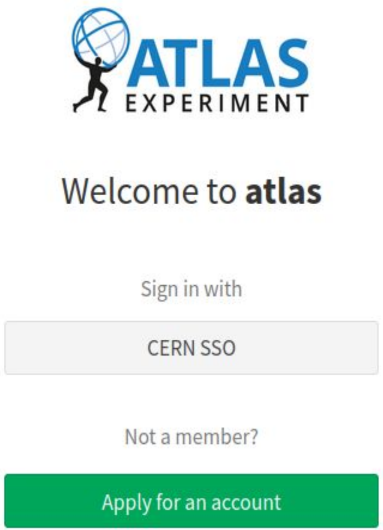
Your Organisation via eduGAIN

Not a member?

Apply for an account

About Us, Contact information and Privacy Policy

iris-iam.stfc.ac.uk



Welcome to **atlas**

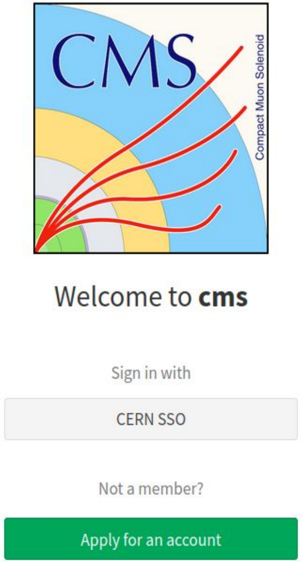
Sign in with

CERN SSO

Not a member?

Apply for an account

atlas-auth.web.cern.ch



Welcome to **cms**

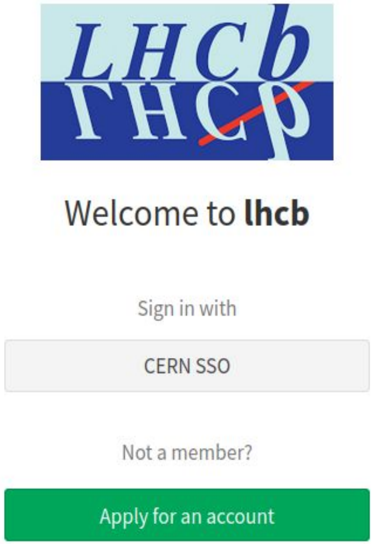
Sign in with

CERN SSO

Not a member?

Apply for an account

cms-auth.web.cern.ch



Welcome to **lhcb**

Sign in with

CERN SSO

Not a member?

Apply for an account

lhcb-auth.web.cern.ch

Welcome to **MesoNET SSO**

Sign in with your MesoNET SSO credentials

Username

Password

Sign in

Forgot your password?

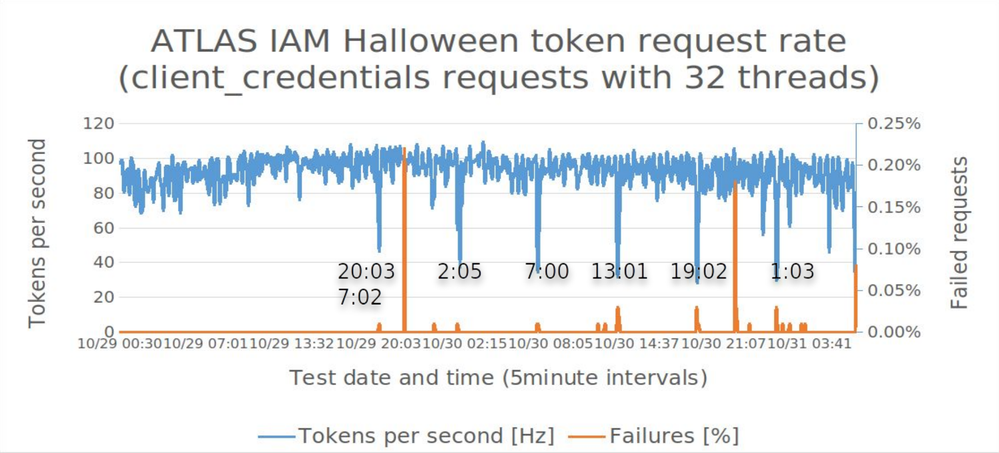
Or sign in with

eduGAIN

iam-mesonet.ijclab.in2p3.fr

IAM performance: a goal to be achieved

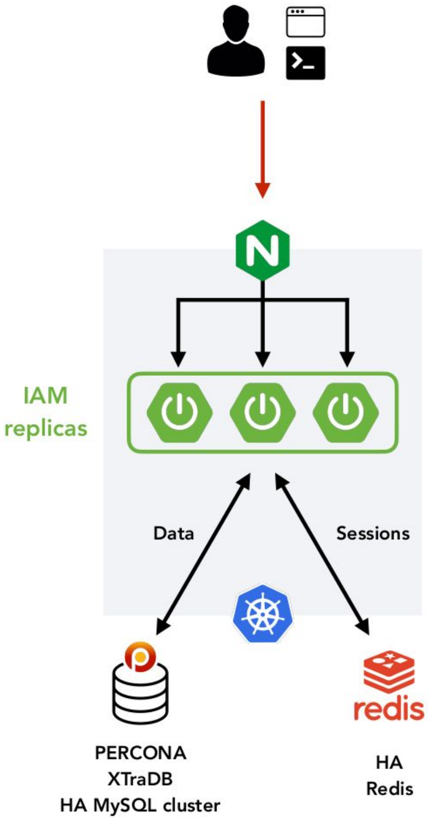
- Unannounced stress tests have been performed on the Atlas IAM instance hosted at CERN
    - `vegeta attack` with 100 Hz token request rate using client credentials grant
- ~100 Hz sustained for more than two days (300 ms response time, 0% error rate)
- then, IAM showed some degradation and it became unavailable due to deployment limits
- Recent stress tests on a CERN instance have shown that IAM can sustain up to 500 Hz just optimizing the NGINX configuration
- **Scalability and performance tests are planned for the next [IAM Hackathon]**



Funded by the European Union's Horizon 2020 - Grant N° 824064

IAM in High Availability

- Starting from version 1.8.0, the IAM service can be deployed in **High Availability** mode
  - IAM supports session data externalization
  - IAM becomes a completely stateless application
- About externalized sessions: IAM relies on redis as external component used to store session data
- Tests in progress: IAM has been deployed with 3 replicas on the dev IAM instance (at CNAF)
  - we faced some cluster limits
  - we planned to use a testbed hosted at CERN



Funded by the European Union's Horizon 2020 - Grant N° 824064

IAM demo

What will be shown

ESCAPE IAM v1.8.1 (current version):

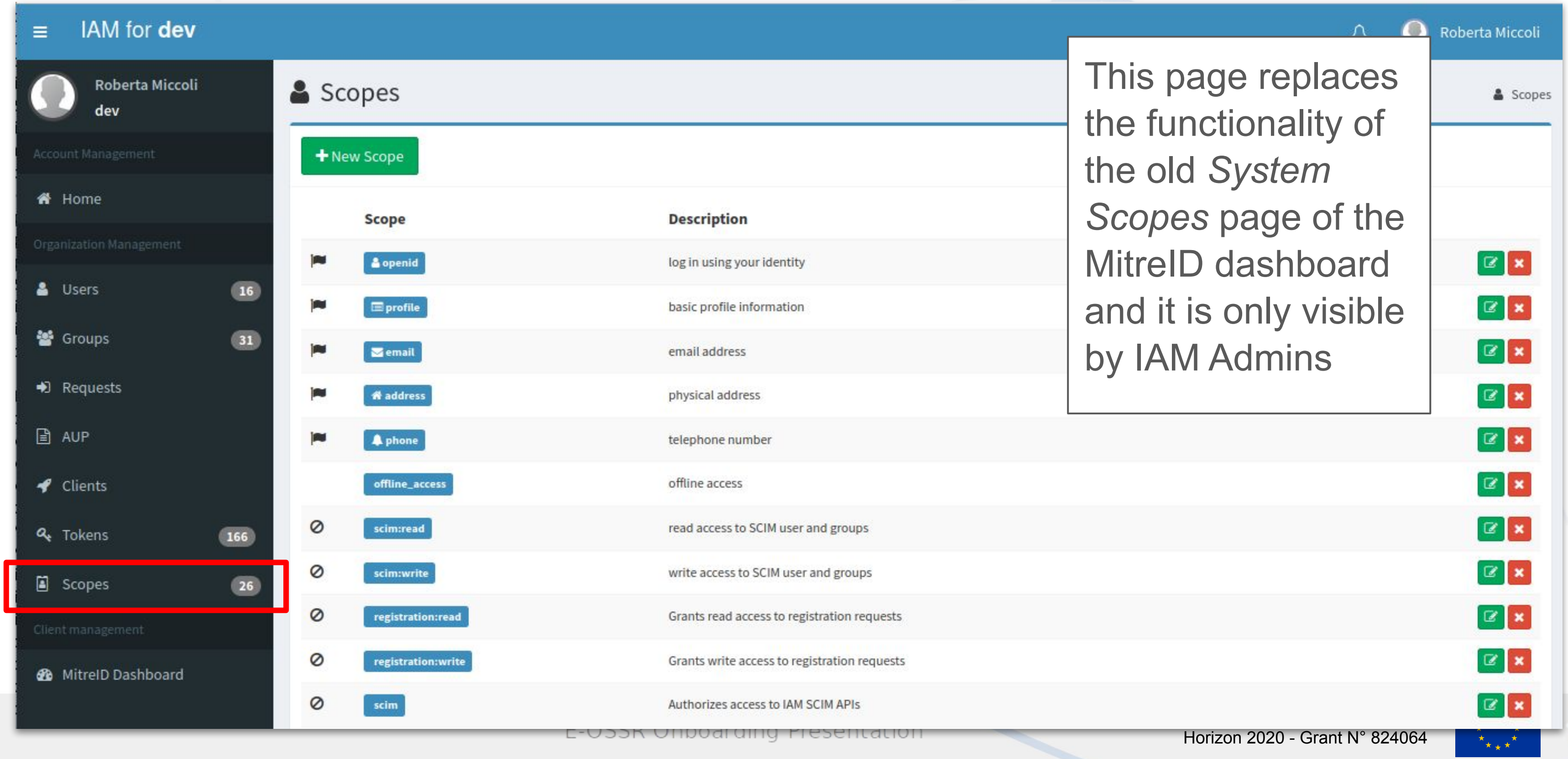
- Scope management interface
- Group Manager interface

ESCAPE IAM v1.8.2 (next version):

- Access to IAM API endpoints requires new admin scopes

Funded by the European Union's
Horizon 2020 - Grant N° 824064

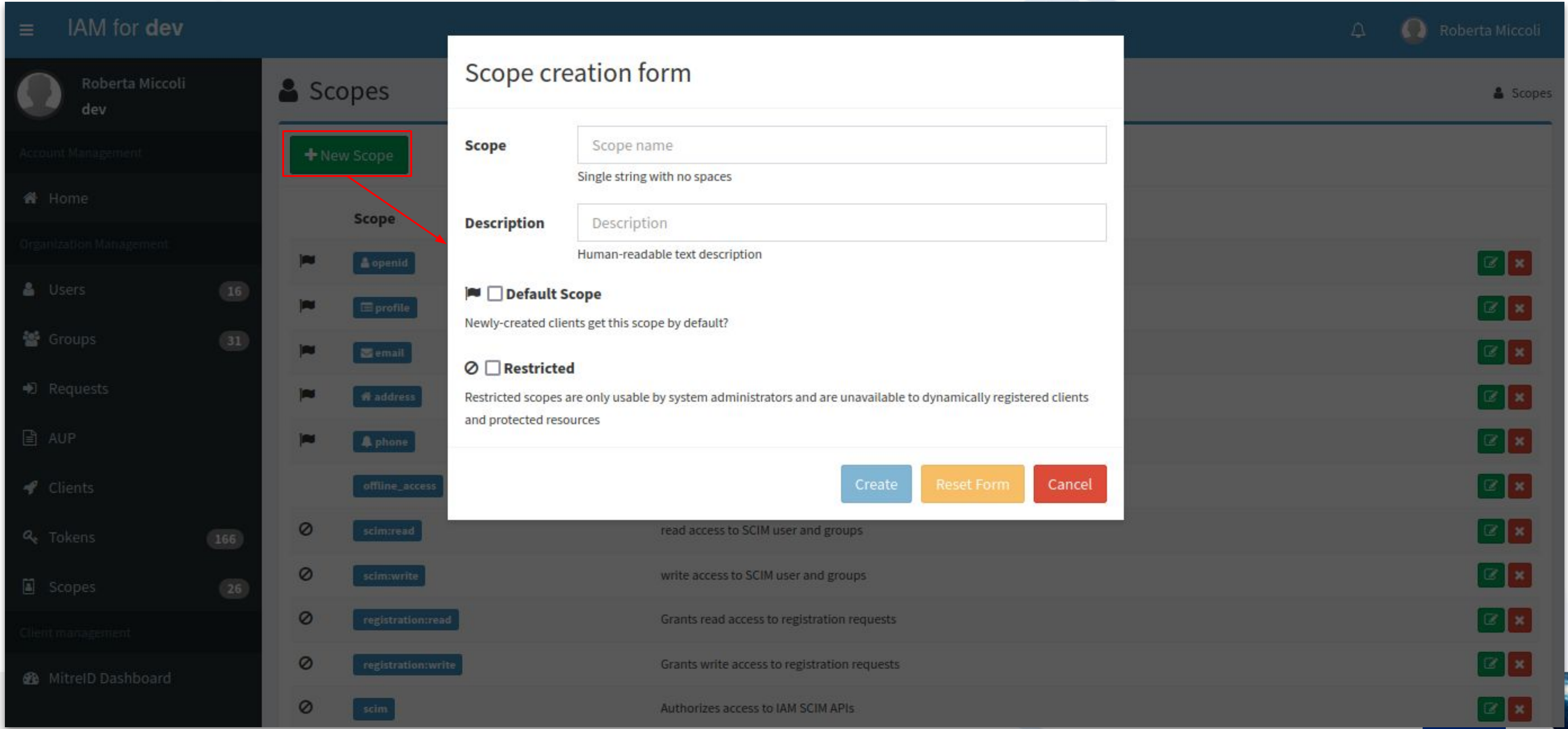
Scopes management interface



	Scope	Description
⚑	openid	log in using your identity
⚑	profile	basic profile information
⚑	email	email address
⚑	address	physical address
⚑	phone	telephone number
	offline_access	offline access
⊘	scim:read	read access to SCIM user and groups
⊘	scim:write	write access to SCIM user and groups
⊘	registration:read	Grants read access to registration requests
⊘	registration:write	Grants write access to registration requests
⊘	scim	Authorizes access to IAM SCIM APIs

This page replaces the functionality of the old *System Scopes* page of the MitreID dashboard and it is only visible by IAM Admins

Scopes management interface



Scope creation form

Scope Scope name

Single string with no spaces

Description Description

Human-readable text description

□ **Default Scope**

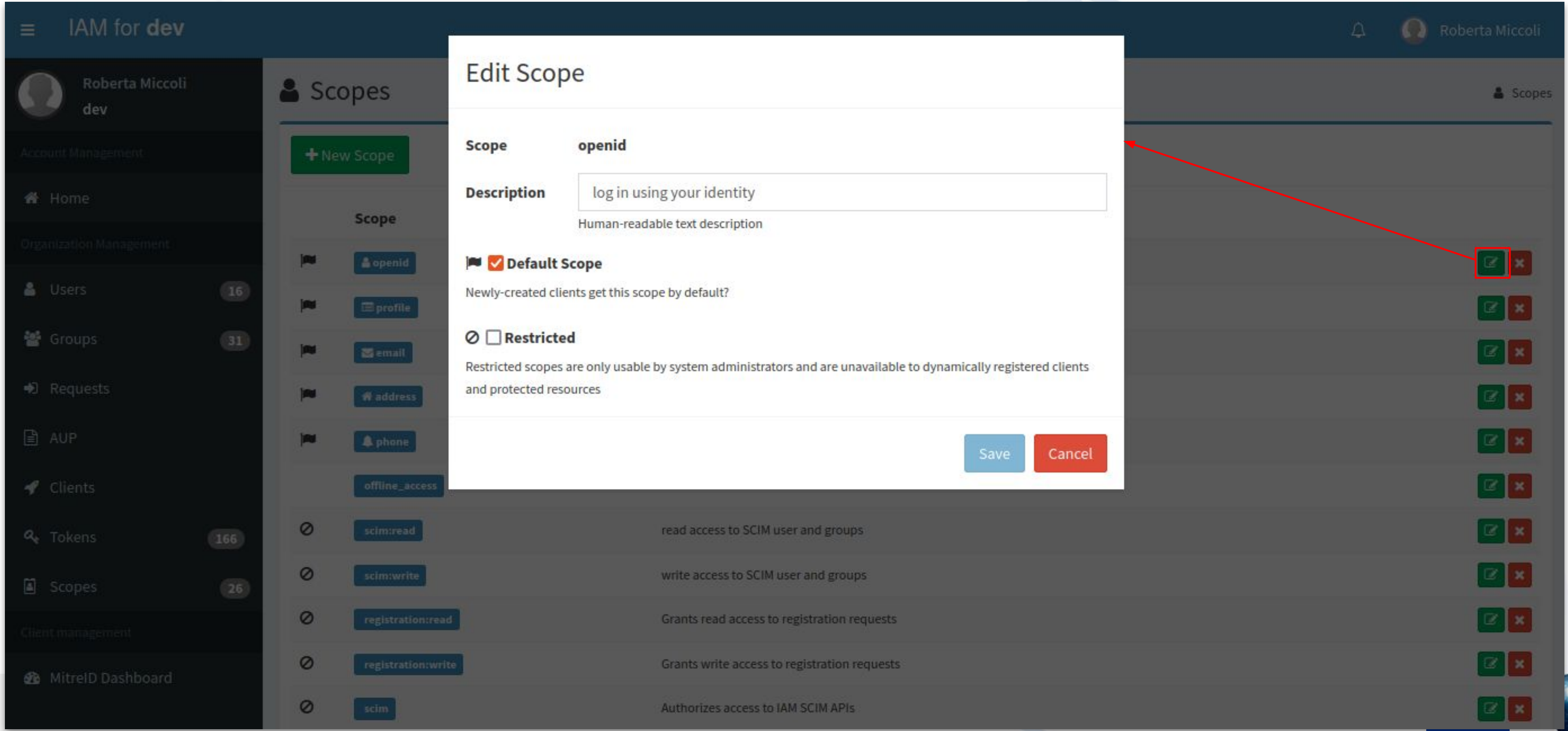
Newly-created clients get this scope by default?

⊘ □ **Restricted**

Restricted scopes are only usable by system administrators and are unavailable to dynamically registered clients and protected resources

	Scope	
⚑	openid	
⚑	profile	
⚑	email	
⚑	address	
⚑	phone	
	offline_access	
⊘	scim:read	read access to SCIM user and groups
⊘	scim:write	write access to SCIM user and groups
⊘	registration:read	Grants read access to registration requests
⊘	registration:write	Grants write access to registration requests
⊘	scim	Authorizes access to IAM SCIM APIs

Scopes management interface



Edit Scope

Scope **openid**

Description log in using your identity

Human-readable text description

⚑ ☑ **Default Scope**

Newly-created clients get this scope by default?

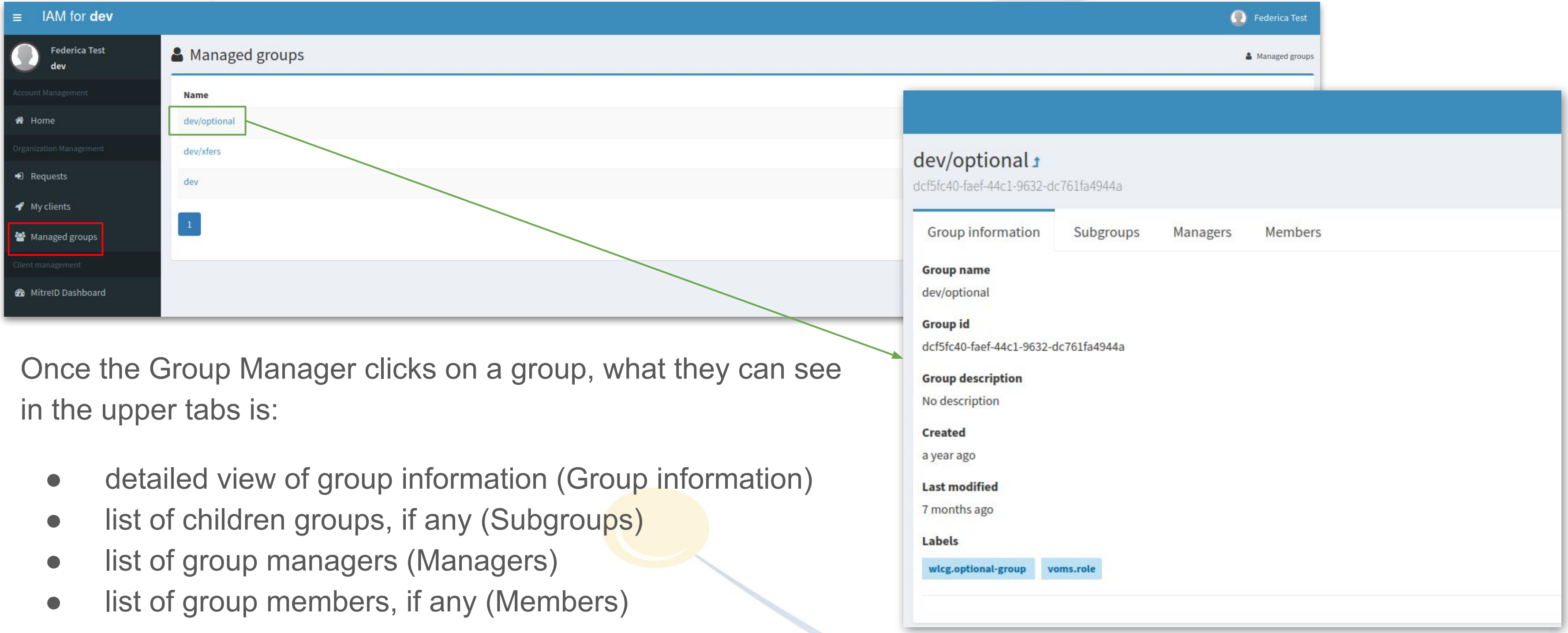
⊘ □ **Restricted**

Restricted scopes are only usable by system administrators and are unavailable to dynamically registered clients and protected resources

Save Cancel

	Scope	
⚑	openid	
⚑	profile	
⚑	email	
⚑	address	
⚑	phone	
	offline_access	
⊘	scim:read	read access to SCIM user and groups
⊘	scim:write	write access to SCIM user and groups
⊘	registration:read	Grants read access to registration requests
⊘	registration:write	Grants write access to registration requests
⊘	scim	Authorizes access to IAM SCIM APIs

Group Manager interface



IAM for **dev**

Federica Test

Federica Test
dev

Account Management
- Home

Organization Management
- Requests
- My clients
- Managed groups

Client management
- MitreID Dashboard

Managed groups

Name
dev/optional
dev/xfers
dev

1

dev/optional
dcf5fc40-faef-44c1-9632-dc761fa4944a

Group information | Subgroups | Managers | Members

Group name
dev/optional

Group id
dcf5fc40-faef-44c1-9632-dc761fa4944a

Group description
No description

Created
a year ago

Last modified
7 months ago

Labels
wlcg.optional-group voms.role

Once the Group Manager clicks on a group, what they can see in the upper tabs is:

- detailed view of group information (Group information)
- list of children groups, if any (Subgroups)
- list of group managers (Managers)
- list of group members, if any (Members)

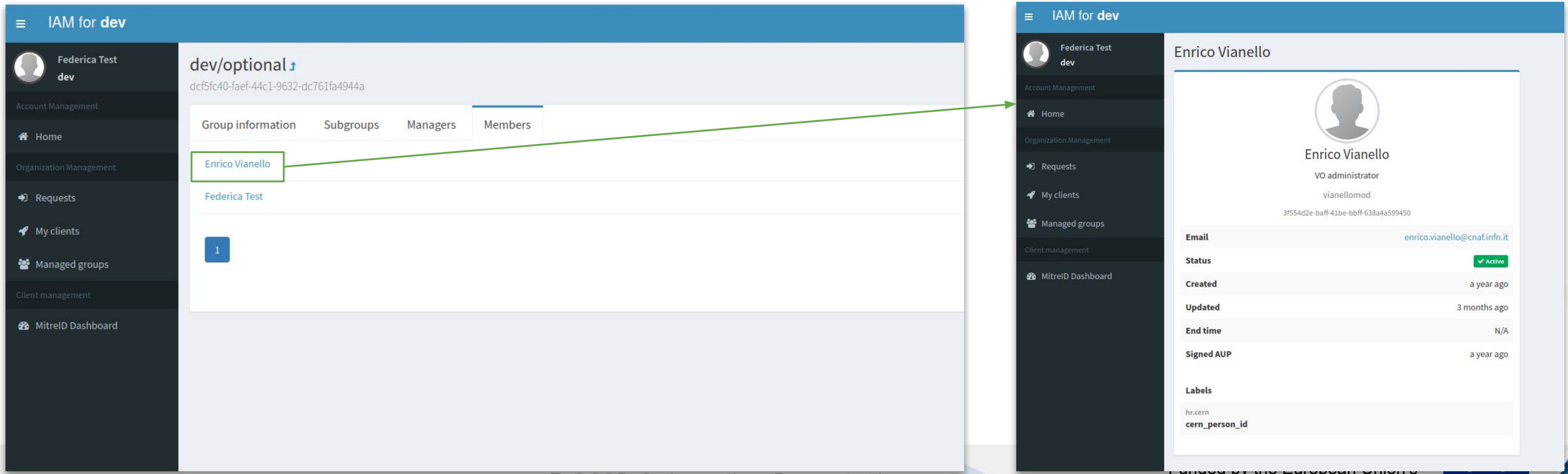
Funded by the European Union's
Horizon 2020 - Grant N° 824064

Group Manager interface

A Group Manager in IAM does not have the same privileges as the IAM Admin in managing groups. Currently, they can:

- approve/reject membership requests
- delete users from their managed groups

The Group Manager has also the possibility to click on group members, where a limited view of user information (including name, surname, uuid, username, email, status, created, updated, end time and labels) is shown.



dev/optional

dcf5fc40-faef-44c1-9632-dc761fa4944a

Enrico Vianello

VO administrator

vianellomod

3f554d2e-baff-41be-bbff-638a4a599450

Email	enrico.vianello@cnaf.infn.it
Status	✓ Active
Created	a year ago
Updated	3 months ago
End time	N/A
Signed AUP	a year ago

Labels

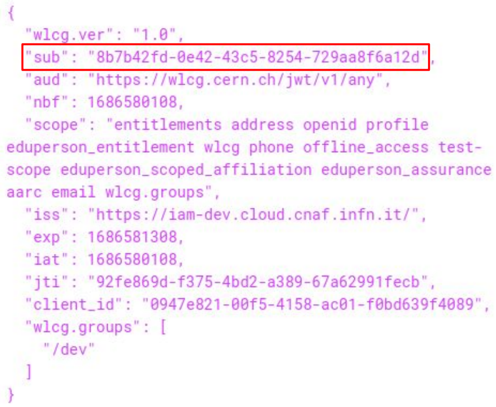
hr.cern
cern_person_id

Funded by the European Union's
Horizon 2020 - Grant N° 824064

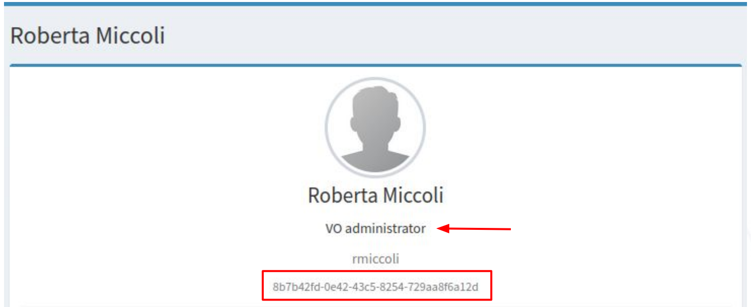
Access to IAM API endpoints

```
$ oidc-token escape-demo
eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJ3bGNnLn…

$ curl -X GET -H "Authorization: Bearer eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJ3bGNnLn…"
https://iam-dev.cloud.cnaf.infn.it/iam/account/search
{"error":"insufficient_scope","error_description":"Insufficient scope for this
resource","scope":"iam:admin.read"}
```



```
{
  "wlcg.ver": "1.0",
  "sub": "8b7b42fd-0e42-43c5-8254-729aa8f6a12d",
  "aud": "https://wlcg.cern.ch/jwt/v1/any",
  "nbf": 1686580108,
  "scope": "entitlements address openid profile
eduperson_entitlement wlcg phone offline_access test-
scope eduperson_scoped_affiliation eduperson_assurance
aarc email wlcg.groups",
  "iss": "https://iam-dev.cloud.cnaf.infn.it/",
  "exp": 1686581308,
  "iat": 1686580108,
  "jti": "92fe869d-f375-4bd2-a389-67a62991fecb",
  "client_id": "0947e821-00f5-4158-ac01-f0bd639f4089",
  "wlcg.groups": [
    "/dev"
  ]
}
```



Roberta Miccoli

Roberta Miccoli

VO administrator

rmiccoli

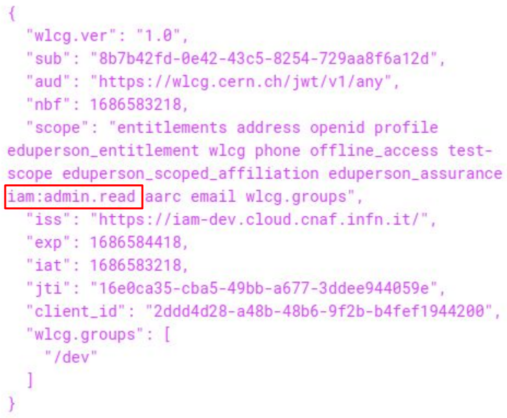
8b7b42fd-0e42-43c5-8254-729aa8f6a12d

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Access to IAM API endpoints

```
$ oidc-token escape-demo2
eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJ3bGNnLnZlciI6Ij…

$ curl -X GET -H "Authorization: Bearer eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJ3bGNnLnZlciI6Ij…"
https://iam-dev.cloud.cnaf.infn.it/iam/account/search | jq
{
  "totalResults": 16,
  "itemsPerPage": 10,
  "startIndex": 1,
  "Resources": [
          {
          "id": "73f16d93-2441-4a50-88ff-85360d78c6b5",
          "meta": {
          "created": "2021-12-08T08:50:13.000+01:00",
          "lastModified": "2021-12-08T08:50:13.000+01:00",
          "location":
"https://iam-dev.cloud.cnaf.infn.it/scim/Users/73f16d93-2441-4a50-88ff-85360d78c6b5",
          "resourceType": "User"
          },
          "userName": "admin",
          "name": {
          "familyName": "User",
          "formatted": "Admin User",
          "givenName": "Admin"
          },
          "displayName": "admin",
          "active": true,
          "emails": [
          {
          "type": "work",
          "value": "admin@iam.test",
          "primary": true
...
```



```
{
  "wlcg.ver": "1.0",
  "sub": "8b7b42fd-0e42-43c5-8254-729aa8f6a12d",
  "aud": "https://wlcg.cern.ch/jwt/v1/any",
  "nbf": 1686583218,
  "scope": "entitlements address openid profile
eduperson_entitlement wlcg phone offline_access test-
scope eduperson_scoped_affiliation eduperson_assurance
iam:admin.read aarc email wlcg.groups",
  "iss": "https://iam-dev.cloud.cnaf.infn.it/",
  "exp": 1686584418,
  "iat": 1686583218,
  "jti": "16e0ca35-cba5-49bb-a677-3ddee944059e",
  "client_id": "2ddd4d28-a48b-48b6-9f2b-b4fef1944200",
  "wlcg.groups": [
    "/dev"
  ]
}
```

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Thanks for your attention!

Questions?

Useful references

IAM on GitHub: https://github.com/indigo-iam/iam

IAM documentation: https://indigo-iam.github.io/docs

IAM in action video: https://www.youtube.com/watch?v=1rZIvJADOnY

For general information:

- OAuth 2.0: https://oauth.net/2/ and OAuth 2.1: https://oauth.net/2.1/
- OpenID Connect: https://openid.net/connect/
- JSON Web Token: https://www.rfc-editor.org/rfc/rfc7519
- OpenID Connect Federation: https://openid.net/specs/openid-connect-federation-1_0.html

Contacts:

- iam-support@lists.infn.it

Funded by the European Union's
Horizon 2020 - Grant N° 824064